Bundesamt
für Sicherheit in der
Informationstechnik

SYS.2.5 Client-Virtualisierung

1. Beschreibung

1.1. Einleitung

Client-Virtualisierung bezeichnet die virtualisierte Bereitstellung von Clients. Sowohl lokal auf einem physischen Client als auch mittels einer (zentralen) Virtualisierungsinfrastruktur können Clients virtualisiert werden. Virtualisierungsinfrastrukturen können genutzt werden, um virtuelle Clients von einem entfernten Arbeitsplatz aus zu bedienen.

Dieser Baustein behandelt den sicheren Einsatz von Client-Virtualisierung mittels einer Virtualisierungsinfrastruktur. Eine Virtualisierungsinfrastruktur umfasst dabei einen oder mehrere physische Virtualisierungsserver gemäß des Bausteins SYS.1.5 *Virtualisierung*. Die einzelnen virtuellen Clients werden auf den jeweiligen Virtualisierungsservern ausgeführt und setzen sich dabei aus den hierfür festgelegten virtuellen Hardware-Ressourcen wie CPU, Arbeitsspeicher und dem zugehörigen Festplatten-Abbild (Image) zusammen. Diese Abbilder werden üblicherweise anhand von Vorlagen (Templates) erzeugt.

Die Benutzenden interagieren hierbei über physische Clients, die sich mittels Terminalserver-Techniken und -Protokollen mit den virtuellen Clients verbinden. Somit ist der virtuelle Client auch ein Terminalserver im Sinne des Bausteins SYS.1.9 *Terminalserver*.

Virtuelle Clients, die auf einer Virtualisierungsinfrastruktur ausgeführt werden, sind in der Regel leichter zu administrieren als physische Clients, die geographisch über die Institution verteilt sind. Weiterhin können virtuelle Clients anhand von Templates einfacher als physische Clients provisioniert werden. Zudem können virtuelle Clients über Snapshots oder geklonte virtuelle Maschinen einfacher aktualisiert werden. Ein anderer typischer Einsatzfall sind virtuelle Clients, die erzeugt werden, um bestimmte Anwendungen zu testen und daher nur für einen kurzen Zeitraum benötigt werden.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, Informationen zu schützen, die bei der Client-Virtualisierung verarbeitet und übertragen werden. Hierzu werden spezielle Anforderungen an die virtuellen Clients und die zugrundeliegende Virtualisierungsinfrastruktur sowie an die verwendeten Netze gestellt.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.2.5 *Client-Virtualisierung* ist auf die Virtualisierungsinfrastruktur sowie alle virtuellen Clients anzuwenden, sofern diese wie oben beschrieben zentral bereitgestellt werden.

Um ein IT-Grundschutz-Modell für einen konkreten Informationsverbund zu erstellen, muss grundsätzlich die Gesamtheit aller Bausteine betrachtet werden. In der Regel sind mehrere Bausteine auf das Thema bzw. Zielobjekt anzuwenden.

Dieser Baustein behandelt die folgenden Inhalte:

- Der Baustein SYS.2.5 *Client-Virtualisierung* thematisiert diejenigen Teile einer Client-Virtualisierung, die spezifisch für die Bereitstellung und den Einsatz von virtuellen Clients sind.
- Dieser Baustein beinhaltet spezifische Anforderungen an die verwendeten Netze, um die Kommunikation zwischen zugreifendem Client und Virtualisierungsinfrastruktur abzusichern.

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:

- Zugreifende und virtuelle Clients kommunizieren über eine Terminalserver-Software, die auf den virtuellen Clients ausgeführt wird. Daher ist der Baustein SYS.1.9 *Terminalserver* sowohl auf die virtuellen Clients als auch auf die zugreifenden Clients anzuwenden.
- Um die allgemeinen Aspekte von virtuellen Clients zu adressieren, ist der Baustein SYS.2.1 *Allgemeiner Client* anzuwenden. Weiterhin sind gegebenenfalls die betriebssystemspezifischen Bausteine der Schicht *SYS* anzuwenden.
- Die allgemeinen Aspekte der Virtualisierung, zum Beispiel die Isolation über den Virtualisierungsserver, werden im Baustein SYS.1.5 *Virtualisierung* adressiert.
- Der Baustein NET.1.1 *Netzarchitektur und –design* muss angewendet werden, um die Netze abzusichern, die für die Kommunikation zwischen zugreifendem Client und Virtualisierungsinfrastruktur genutzt werden.

Dieser Baustein behandelt **nicht** die folgenden Inhalte:

- Die lokale Bereitstellung von virtuellen Clients auf physischen Clients.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.2.5 *Client-Virtualisierung* von besonderer Bedeutung.

2.1. Unzureichende Dimensionierung der Netzanbindung virtueller Clients

Werden bei der Planung der virtuellen Clients die Leistungsanforderungen an deren Netzanbindung nicht oder nur unzureichend berücksichtigt, könnten die virtuellen Clients nicht richtig funktionieren. Ist beispielsweise die Netzanbindung an nachgelagerte Dienste (z. B. Videokonferenzlösungen oder Dateiablagen) nicht leistungsfähig genug, können die virtuellen Clients unter Umständen nur noch eingeschränkt auf Informationen zugreifen, z. B. bei latenzkritischen Anwendungen. Ähnliches gilt, wenn die virtuellen Clients nicht mit hinreichender Netzkapazität an die zugreifenden Clients angebunden sind.

2.2. Unzureichende Leistung der virtuellen Clients durch Ressourcenknappheit

Um auf virtuellen Clients möglichst reibungslos arbeiten zu können, ist es wichtig, dass sie leistungsfähig sind. Werden einem virtuellen Client nur unzureichende Ressourcen (z. B. CPU, Arbeitsspeicher oder Grafikleistung) zugewiesen, kann die Verfügbarkeit der auf dem virtuellen Client installierten Anwendungen beeinträchtigt werden. Beispielsweise können bestimmte grafisch anspruchsvolle Programme nicht ohne dedizierte Grafikprozessoren auf dem virtuellen Client ausgeführt werden. Auch ein zu niedriger Prozessortakt führt zu einer langsamen Verarbeitungsgeschwindigkeit.

Verhalten sich die virtuellen Clients unterschiedlich, können hierdurch Ressourcen knapp werden. Führen Benutzende beispielsweise viele Anwendungen dauerhaft und parallel aus, können die virtuellen Clients unter Umständen die erforderliche Leistung nicht mehr erbringen.

2.3. Gegenseitiges Stören der virtuellen Clients

Die Dimensionierung der zugrundeliegenden Virtualisierungsinfrastruktur ist maßgeblich für die tatsächlich abrufbare Leistung mehrerer parallel ausgeführter virtueller Clients. Werden auf einem Virtualisierungsserver zusätzlich zu einem virtuellen Client viele andere virtuelle IT-Systeme gleichzeitig ausgeführt, könnte der Virtualisierungsserver den Ressourcenbedarf nicht mehr decken. Dies wiederum kann dazu führen, dass die tatsächliche Leistung des virtuellen Clients begrenzt und nicht mehr vorhersehbar wird. Prozessorleistung und Arbeitsspeicher spielen dabei die größte Rolle, wenn sie dynamisch zugewiesen werden. Rufen nun zu viele verschiedene Personen zeitgleich Leistung ab, konkurrieren sie um diese.

Besonders wenn virtuelle Clients unsachgemäß benutzt werden und die bereitgestellten Ressourcen stark ausgelastet sind, können andere virtuelle Clients beeinträchtigt werden. Im Extremfall kann der zugrundeliegende Virtualisierungsserver ein virtuelles IT-System aus Ressourcenmangel beenden oder sogar selbst vollständig ausfallen.

2.4. Unzureichende Trennung der virtuellen Clients auf Netzebene

Bei den virtuellen Clients handelt es sich um Clients im Sinne des Bausteins SYS.2.1 *Allgemeiner Client*, die gegebenenfalls einen unterschiedlichen Schutzbedarf haben können. Werden diese Clients auf einer gemeinsamen Virtualisierungsinfrastruktur betrieben, könnte eine bestehende Trennung auf Port-Ebene durch den eingesetzten Virtualisierungsserver aufgehoben werden (auf Ebene der virtuellen Switches).

Werden die virtuellen Clients, z. B. durch Konfigurationsfehler, auf Ebene der virtuellen Switches, VLANs oder physischen Schnittstellen nicht den vorgesehenen Netzsegmenten zugeordnet, könnten diese auf schützenswerte Netze und dort befindliche Informationen zugreifen, für die sie nicht berechtigt sind.

Virtualisierungsserver werden in der Regel in zentralen IT-Betriebsbereichen (Rechenzentren) betrieben, in denen auch weitere zentrale Server positioniert sind. Sind virtuelle Clients und zentrale Server nicht in Netzsegmenten positioniert, die voneinander getrennt sind, können virtuelle Clients unberechtigt oder unbeabsichtigt auf Server zugreifen. Sind in diesen Netzsegmenten virtuelle Clients enthalten, die auf das Internet zugreifen dürfen, vergrößert dies die Angriffsfläche.

2.5. Verlust von virtuellen Clients und darauf gespeicherten Daten

Bei der Client-Virtualisierung werden die Images der virtuellen Clients an zentraler Stelle gespeichert und verwaltet. Durch fehlerhafte Administration oder Fehlbedienung von virtuellen Clients können diese beschädigt oder gelöscht werden. Der Verlust virtueller Clients im laufenden Betrieb kann dazu führen, dass auch Informationen gelöscht werden, die auf diesen virtuellen Clients gespeichert sind. Zusätzlich bedeutet der Verlust virtueller Clients, dass Informationen, die auf diesen virtuellen Clients verarbeitet werden, nicht mehr verfügbar sind.

2.6. Nicht-Erreichbarkeit von virtuellen Clients und darauf gespeicherten Daten

In der Regel können virtuelle Clients nicht von den Benutzenden selber eingeschaltet werden, sondern nur vom IT-Betrieb, der auch die Virtualisierungsinfrastruktur administriert. Bei Updates oder generell Wartungsarbeiten an der Virtualisierungsinfrastruktur ist es üblich, dass virtuelle Clients ausgeschaltet werden. Wird vergessen, sie hinterher wieder einzuschalten, bleiben sie ausgeschaltet und sind somit nicht erreichbar.

Ebenso kann ein Ausfall des zugrundeliegenden Virtualisierungsservers dazu führen, dass virtuelle Clients temporär nicht erreichbar sind. In diesem Fall können die Benutzenden nicht mehr auf den jeweiligen virtuellen Client und die darauf gespeicherten Daten zugreifen.

2.7. Software-Schwachstellen auf den virtuellen Clients

Virtuelle Clients setzen sich aus den festgelegten virtuellen Hardware-Ressourcen wie CPU und Arbeitsspeicher und dem zugehörigen Festplatten-Abbild zusammen. Diese Abbilder werden üblicherweise anhand von Vorlagen erzeugt. Wenn diese Vorlagen erzeugt werden, sind sie in der Regel auf einem aktuellen Software-Stand ohne bekannte Schwachstellen.

Ohne eine regelmäßige Aktualisierung dieser Vorlagen ist es jedoch möglich, dass ein neu erzeugter virtueller Client Schwachstellen aufweist, die bekannt wurden, nachdem die Vorlage erzeugt wurde. Können andere IT-Systeme auf diesen virtuellen Client zugreifen, kann die bekannte Schwachstelle unter Umständen ausgenutzt werden und somit der virtuelle Client kompromittiert werden.

Auch kann es notwendig sein, virtuelle Clients mit bekannten Schwachstellen zu provisionieren, z. B. für Kompatibilitätstests oder für benötigte Software, die nur auf veralteten Betriebssystemen lauffähig ist. Diese Schwachstellen können vorhersehbar auftreten und so leichter ausgenutzt werden.

2.8. Umgehen der Isolation zwischen einem virtuellen Client und anderen virtualisierten IT-Systemen

Virtuelle IT-Systeme werden oft auf einer gemeinsam genutzten Virtualisierungsinfrastruktur eingesetzt, um Ressourcen effizienter zu nutzen und flexibler bereitzustellen. Dadurch können sich die verschiedenen virtualisierten IT-Systeme gegenseitig beeinflussen. Im Gegensatz zu einem virtuellen Server können virtuelle Clients einfacher kompromittiert werden, da die auf den virtuellen Clients ausgeführten Anwendungen vielfältiger und interaktiver sind.

Ein kompromittierter virtueller Client kann die gemeinsam genutzte Virtualisierungsinfrastruktur gefährden, da nicht nur über das Netz erreichbare IT-Systeme, sondern auch andere virtuelle IT-Systeme auf dem Virtualisierungsserver angegriffen werden können. Da das physische IT-System gemeinsam genutzt wird, können beispielsweise Seitenkanalangriffe wie Spectre oder Meltdown durchgeführt oder es kann aus der virtuellen Maschine ausgebrochen werden, um anschließend den zugrundeliegenden Hypervisor oder das zugrundeliegende Betriebssystem zu kompromittieren. In diesem Fall können virtuelle IT-Systeme außer Betrieb genommen oder auch die in ihnen verarbeiteten Daten ausgelesen oder modifiziert werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.2.5 *Client-Virtualisierung* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Planende

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.2.5.A1 Planung des Einsatzes virtueller Clients (B)

Es MUSS festgelegt werden, welche Anwendungen auf den virtuellen Clients eingesetzt werden sollen. Die Aufgaben, die mit diesen Anwendungen gelöst werden sollen, MÜSSEN festgelegt werden. Für diese Anwendungen MUSS überprüft und dokumentiert werden, welche Anforderungen an die Virtualisierungsinfrastruktur und deren etwaige Zusatzhardware (z. B. Grafikkarten) gestellt werden. Der genutzte Virtualisierungsserver MUSS die notwendigen Ressourcen hinsichtlich CPU, Arbeitsspeicher und Datenspeicher bereitstellen.

SYS.2.5.A2 Planung der verwendeten Netze für virtuelle Clients (B) [Planende]

Die Netze für die Verbindung zwischen zugreifenden Clients und virtuellen Clients sowie die Netze zur Anbindung nachgelagerter Dienste an die virtuellen Clients (z. B. Verzeichnisdienst, E-Mail oder Internetzugriff) MÜSSEN ausreichend leistungsfähig ausgelegt werden.

Es MUSS geplant werden, welche Netzsegmente für die virtuellen Clients verwendet werden sollen. Die Netzsegmente für virtuelle Clients MÜSSEN von Netzsegmenten für Server getrennt sein. Eine bestehende Netztrennung DARF NICHT mithilfe eines virtuellen Clients oder eines Virtualisierungsservers umgangen werden.

Für virtuelle Clients MUSS festgelegt werden, ob und in welchem Ausmaß die Kommunikation in nicht vertrauenswürdige Netze eingeschränkt werden soll.

SYS.2.5.A3 Schutz vor Schadsoftware auf den virtuellen Clients (B)

Für die virtuellen Clients MUSS ein Schutz vor Schadsoftware gemäß den Bausteinen OPS.1.1.4 *Schutz vor Schadprogrammen* und SYS.2.1 *Allgemeiner Client* sowie unter Berücksichtigung der betriebssystemspezifischen Bausteine umgesetzt werden. Wird ein Virenschutzprogramm eingesetzt, MUSS festgelegt und dokumentiert werden, ob dieser Schutz zentralisiert in der Virtualisierungsinfrastruktur, dezentralisiert auf den virtuellen Clients oder in Mischformen umgesetzt wird. Falls die virtuellen Clients mit zentralen Komponenten geschützt werden sollen, MÜSSEN diese zentralen Komponenten über eine ausreichende Leistung verfügen.

Falls ein Virenschutzprogramm auf den virtuellen Clients ausgeführt wird, MUSS sichergestellt werden, dass die Leistung der Virtualisierungsinfrastruktur ausreicht.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.2.5.A4 Verwendung einer dedizierten Virtualisierungsinfrastruktur für die virtuellen Clients (S)

Die virtuellen Clients SOLLTEN auf einer dedizierten Virtualisierungsinfrastruktur betrieben werden. Virtuelle Server SOLLTEN NICHT auf derselben Virtualisierungsinfrastruktur ausgeführt werden.

SYS.2.5.A5 Zusätzliche Netzsegmentierung für virtuelle Clients (S)

Folgende Kriterien SOLLTEN für eine zusätzliche Netztrennung der virtuellen Clients berücksichtigt werden:

- Nutzungsszenario für die virtuellen Clients und Gruppenzugehörigkeit der Benutzenden
- aus der Gruppenzugehörigkeit abgeleitete Berechtigungen der Benutzenden
- auf den virtuellen Clients installierte und den Benutzenden zur Verfügung gestellte Anwendungen
- Schutzbedarf der auf den virtuellen Clients verarbeiteten Informationen
- Vertrauenswürdigkeit der virtuellen Clients
- für die Funktionsfähigkeit der virtuellen Clients notwendige Netzanbindungen

SYS.2.5.A6 Keine lokale Datenablage auf virtuellen Clients (S)

Durch die Benutzenden erstellte oder verarbeitete Daten SOLLTEN zentral gespeichert werden. Die Daten SOLLTEN NICHT dauerhaft auf den virtuellen Clients abgelegt werden.

Benutzende, die sich mit virtuellen Clients verbinden, SOLLTEN NICHT in der Lage sein, Daten aus den virtuellen Clients auf ihre lokalen IT-Systeme zu übertragen. Falls eine solche Übertragung nachvollziehbar notwendig ist, SOLLTE sie auf das notwendige Minimum beschränkt werden.

SYS.2.5.A7 Automatische Sperrung von Sitzungen (S)

Nachdem ein zugreifender Client seine Terminalserver-Sitzung beendet hat, SOLLTE die aktive Sitzung auf dem virtuellen Client gesperrt werden. Nach einer definierten Zeit der Inaktivität SOLLTEN Verbindungen zwischen zugreifendem und virtuellem Client beendet werden. Falls der Einsatzzweck des jeweiligen virtuellen Clients dies zulässt, SOLLTEN die virtuellen Clients in einen inaktiven Zustand versetzt werden, nachdem die Verbindung beendet ist.

SYS.2.5.A8 Härtung der virtuellen Clients (S)

Die virtuellen Clients SOLLTEN gehärtet werden. Hierbei SOLLTEN die folgenden Aspekte berücksichtigt werden:

- Einschränkung der Datenübertragung zwischen zugreifenden und virtuellen Clients
- Weiterleitungen von Peripheriegeräten oder externen Datenträgern von zugreifenden an die virtuellen Clients
- Explizite Freigabe der Ausführung von Anwendungen
- Deaktivierung von Netzdiensten, die in der Virtualisierungsinfrastruktur nicht benötigt werden

SYS.2.5.A9 Einbindung der virtuellen Clients in das Patch- und Änderungsmanagement (S)

Die Client-Anwendungen SOLLTEN zentral provisioniert werden. Dazu SOLLTE eine geeignete zentral verwaltbare Lösung eingesetzt werden. Templates für die virtuellen Clients SOLLTEN regelmäßig aktualisiert und getestet werden.

SYS.2.5.A10 Bedarfsgerechte Zuweisung von Ressourcen zu virtuellen Clients und Gruppen (S)

Anhand von Rollen und Tätigkeiten SOLLTEN die Leistungsanforderungen der einzelnen Benutzendengruppen an die virtuellen Clients identifiziert werden. Anhand dieser Anforderungen SOLLTE entschieden werden, wie viele Ressourcen (z. B. Prozessorkerne oder Arbeitsspeicher) den einzelnen virtuellen Clients zur Verfügung gestellt werden.

Zusätzliche Ressourcen wie GPUs (Graphics Processing Units) SOLLTEN den Benutzenden nur bei Bedarf bereitgestellt werden.

SYS.2.5.A11 Vermeidung von verschachtelter Virtualisierung auf virtuellen Clients (S)

Auf virtuellen Clients SOLLTEN keine weiteren virtuellen IT-Systeme eingerichtet werden. Falls technisch möglich, SOLLTEN in der zugrundeliegenden Virtualisierungsinfrastruktur Funktionen aktiviert werden, die eine verschachtelte Virtualisierung erschweren oder unterbinden.

SYS.2.5.A12 Sensibilisierung der Benutzenden (S)

Alle Benutzenden von virtuellen Clients SOLLTEN über den sicheren Umgang mit virtuellen Clients sensibilisiert werden. Falls die Ressourcen dynamisch anhand der abgerufenen Leistung zwischen mehreren virtuellen Clients aufgeteilt werden, SOLLTEN die Benutzenden darüber aufgeklärt werden, dass ihr Verhalten potenziell andere Benutzende beeinflussen kann.

Falls die Sicherheitsanforderungen der auf virtuellen Clients ausgeführten Anwendungen besonders sind, SOLLTE kommuniziert werden, wie diese gegenüber physischen Clients abweichen. Es SOLLTE auch kommuniziert werden, welche spezifischen Sicherheitsaspekte zu beachten sind.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.2.5.A13 Verhinderung der Kommunikation zwischen virtuellen Clients an einem gemeinsam genutzten virtuellen Switch (H)

Mechanismen SOLLTEN aktiviert werden, die eine unkontrollierte Layer-2-Kommunikation zwischen virtuellen Clients an einem gemeinsam genutzten virtuellen Switch unterbinden.

SYS.2.5.A14 Erweiterte Sicherheitsfunktionen für den Einsatz von virtuellen Clients (H)

Die virtuellen Clients SOLLTEN mit zusätzlichen Sicherheitsfunktionen geschützt werden. Dabei SOLLTEN mindestens die folgenden Techniken berücksichtigt werden:

- Mikrosegmentierung für die virtuellen Clients
- Intrusion-Detection- oder Intrusion-Prevention-Systeme, die entweder zentralisiert auf der Virtualisierungsinfrastruktur oder dezentral auf den virtuellen Clients bereitgestellt werden

SYS.2.5.A15 Monitoring der virtuellen Clients (H)

Der Zustand der virtuellen Clients SOLLTE zentral überwacht werden. Folgende Parameter SOLLTEN mindestens überwacht werden:

- Erreichbarkeit der virtuellen Clients über alle vorgesehenen Netzschnittstellen,
- Auslastung von CPU und Arbeitsspeicher der virtuellen Clients,
- freie Festplattenkapazität der virtuellen Clients sowie
- Verfügbarkeit der für den Zugriff eingesetzten Terminalserver-Dienste.

Für das Monitoring SOLLTEN vorab die jeweiligen Schwellwerte ermittelt werden (Baselining). Diese Schwellwerte SOLLTEN regelmäßig überprüft und bei Bedarf angepasst werden.

SYS.2.5.A16 Erweiterte Protokollierung für virtuelle Clients (H)

Für virtuelle Clients SOLLTEN zusätzliche Ereignisse an eine zentrale Protokollierungsinfrastruktur (siehe OPS.1.1.5 *Protokollierung*) übermittelt werden. Hierbei SOLLTEN mindestens die folgenden Ereignisse protokolliert werden:

- Aktionen, die mit administrativen Rechten ausgeführt werden,
- Konfigurationsänderungen,
- Installation von Software,
- erfolgreiche und fehlgeschlagene Updates und
- alle Ereignisse, die durch den Schutz vor Schadsoftware entstehen.

SYS.2.5.A17 Erweitertes Monitoring der virtuellen Clients (H)

Die virtuellen Clients SOLLTEN kontinuierlich darauf überwacht werden, ob die in SYS.2.5.A16 *Erweiterte Protokollierung für virtuelle Clients* beschriebenen Ereignisse auftreten. Wird ein Security Information and Event Management (SIEM) genutzt, SOLLTEN die virtuellen Clients darin eingebunden werden. Im SIEM SOLLTEN die überwachten Ereignisse auf Anomalien inklusive Angriffsmustern automatisiert analysiert werden.

Die virtuellen Clients SOLLTEN automatisch und regelmäßig auf Schwachstellen überprüft werden.

SYS.2.5.A18 Hochverfügbare Bereitstellung der Virtualisierungsinfrastruktur (H)

Die virtuellen Clients SOLLTEN hochverfügbar bereitgestellt werden. Dies SOLLTE durch die zugrundeliegende Virtualisierungsinfrastruktur sichergestellt werden. Die Virtualisierungsserver SOLLTEN redundant an die relevanten Netze angeschlossen werden. Bei Ressourcenknappheit SOLLTEN die virtuellen Clients automatisch zwischen den Virtualisierungsservern migriert werden. Bei Ausfall eines Virtualisierungsservers SOLLTEN die virtuellen Clients automatisiert auf einem anderen Virtualisierungsserver gestartet werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein SYS.2.5 *Client-Virtualisierung* sind keine weiterführenden Informationen vorhanden.

Bundesamt
für Sicherheit in der
Informationstechnik

SYS.2.6 Virtual Desktop Infrastructure

1. Beschreibung

1.1. Einleitung

Eine Virtual Desktop Infrastructure (VDI) steuert und verwaltet standardisierte virtuelle Clients. Hierdurch können zentralisiert einzelne Anwendungen (z. B. Office-Programme) oder ganze Desktops zur Verfügung gestellt werden. Virtuelle Clients sind dabei virtualisierte IT-Systeme, auf die über Terminalserver-Protokolle zugegriffen werden kann. Die virtuellen Clients werden auf Virtualisierungsservern ausgeführt, die mit einem Managementsystem zu einer Virtualisierungsinfrastruktur zusammengefasst werden (siehe Bausteine SYS.1.5 *Virtualisierung* und SYS.2.5 *Client-Virtualisierung*).

Je nachdem, welches Produkt eingesetzt wird, besteht eine VDI typischerweise aus Zugangs-, Steuerungs- und Managementkomponenten, die auf einem oder auf mehreren IT-Systemen verteilt betrieben werden. Diese zentralen VDI-Komponenten verwalten unter anderem die Virtualisierungsinfrastruktur und stellen die Verbindungen zwischen zugreifenden und virtuellen Clients her. Daher sind die Virtualisierungsinfrastruktur, die angebundenen Storage-Systeme sowie die virtuellen und zugreifenden Clients ebenfalls impliziter Teil der VDI. In diesem Baustein sind jedoch mit „VDI-Komponenten" immer die folgenden drei zentralen Komponenten einer VDI gemeint:

- Die VDI-Zugangskomponenten authentisieren die Benutzenden und entscheiden anhand ihrer Berechtigungen, ob Zugriffe erlaubt oder nicht erlaubt sowie für welchen Typ von virtuellem Client die Benutzenden autorisiert sind.
- Die VDI-Steuerungskomponenten wählen für die erlaubten Zugänge die entsprechenden virtuellen Clients aus und stellen die Verbindung zwischen zugreifendem und virtuellem Client her.
- Die VDI-Managementkomponenten verwalten die Regeln (z. B. die Zuordnung von Benutzenden zu Clienttypen) und Einstellungen (z. B. die zu nutzenden Protokolle). Außerdem verwalten sie die virtuellen Clients (gemäß SYS.2.5 *Client-Virtualisierung*). Dies umfasst auch die zugewiesenen Ressourcen und deren Provisionierung sowie die Terminalserver-spezifischen Einstellungen der virtuellen Clients.

Außerdem kann es zusätzlich erforderlich sein, dass weitere Infrastrukturdienste angebunden werden, die nicht zur VDI-Lösung selbst gehören (z. B. Verzeichnisdienste, Namensauflösung oder IP-Adress-Management).

VDIs werden in der Regel eingesetzt, um zentral administrierbare standardisierte Arbeitsplätze effizient zur Verfügung zu stellen. Dies wird beispielsweise genutzt, um klassische physische Clients durch Thin Clients zu ersetzen.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, Informationen zu schützen, die beim Einsatz einer VDI gespeichert, verarbeitet und übertragen werden. Hierzu werden spezielle Anforderungen an die in der Einleitung beschriebenen Komponenten einer VDI gestellt.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.2.6 *Virtual Desktop Infrastructure* ist auf jedes IT-System anzuwenden, das als Teil einer VDI-Lösung eingesetzt wird.

Dieser Baustein behandelt die folgenden Inhalte:

Der Baustein SYS.2.6 *Virtual Desktop Infrastructure* behandelt den sicheren Einsatz einer VDI. Dabei wird der Fokus auf die drei zentralen Komponenten einer VDI gelegt.

Dieser Baustein beinhaltet spezifische Anforderungen an die verwendeten Netze, um die Kommunikation zwischen zugreifendem Client und Virtualisierungsinfrastruktur abzusichern.

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:

- Die grundlegende Funktionalität der Kommunikation zwischen einem zugreifenden und einem virtuellen Client in einer VDI-Lösung wird mithilfe von Terminalserver-Techniken erfüllt. Daher ist der Baustein SYS.1.9 *Terminalserver* ebenfalls auf die VDI-Lösung anzuwenden, wobei die einzelnen virtuellen Clients die eigentlichen Terminalserver sind.
- Ebenfalls sind die Bausteine SYS.2.5 *Client-Virtualisierung* und SYS.1.5 *Virtualisierung* für die einzelnen virtuellen Clients bzw. die Virtualisierungsinfrastruktur anzuwenden, speziell für die Isolation der virtuellen Clients über den Virtualisierungsserver.
- Grundsätzliche Anforderungen an die einzelnen Server-Komponenten sowie die zugreifenden und virtuellen Clients sind dem Baustein SYS.1.1 *Allgemeiner Server* bzw. SYS.2.1 *Allgemeiner Client* zu entnehmen. Außerdem sind gegebenenfalls betriebssystemspezifische Bausteine anzuwenden.
- Der Baustein NET.1.1 *Netzarchitektur und –design* muss angewendet werden, um die Netze abzusichern, die für die VDI genutzt werden.

Dieser Baustein behandelt **nicht**

- diejenigen IT-Systeme, die im Kontext der VDI zusätzlich zu den oben beschriebenen VDI-Komponenten verwendet werden (z. B. Storage Systeme) sowie
- die Techniken, die bei der Virtualisierung oder für die Kommunikation zwischen zugreifenden und virtuellen Clients eingesetzt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.2.6 *Virtual Desktop Infrastructure* von besonderer Bedeutung.

2.1. Qualitätsverlust der Bereitstellung virtueller Clients

Eine VDI wird in vielen Fällen dazu eingesetzt, um Ressourcen zu optimieren. Werden jedoch viele virtuelle Clients auf einzelnen Virtualisierungsservern platziert, können die verfügbaren Ressourcen überbucht werden. Auch wenn die geplante Anzahl der Benutzenden unzutreffend eingeschätzt wurde, können die Ressourcen überbucht werden.

Hierdurch können virtuelle Clients in der VDI stark um Ressourcen konkurrieren und die Leistung kann unvorhersehbar einbrechen. Das kann dazu führen, dass die virtuellen Clients temporär nicht mehr verfügbar sind.

Die Leistungseinbrüche sind für die Benutzenden meist intransparent, so dass Daten verloren gehen oder ungewollt geändert werden.

2.2. Falsche Zuweisung von virtuellen Clients zu Benutzenden

Den Benutzenden werden virtuelle Clients und deren Ressourcen anhand von Profilen von der VDI zentralisiert zugewiesen. Sollte eine solche Zuweisung fehlerhaft sein, können hierdurch

- hohe Kosten entstehen, wenn leistungsstarke virtuelle Clients an Benutzende ohne großen Ressourcenbedarf zugewiesen werden,
- virtuelle Clients mit geringer Leistung an Benutzende mit hohem Ressourcenbedarf oder besonderen Hardwareanforderungen, z. B. für CAD-Aufgaben, zugewiesen werden,
- Benutzende auf IT-Systeme und Informationen unberechtigt zugreifen oder
- externe USB-Geräte angebunden und Informationen an nicht dafür vorgesehene virtuelle Clients übertragen werden.

2.3. Unzureichende Netztrennung durch Fehlkonfiguration in der VDI

Typischerweise werden in einer VDI-Lösung unterschiedliche virtuelle Clients betrieben, die sich stark in ihren Anwendungsbereichen unterscheiden und entsprechend auch unterschiedlichen Netzen zugeordnet sein können. Die VDI-Managementkomponente verwaltet alle diese Clients. Ist die VDI-Managementkomponente fehlerhaft konfiguriert, kann eine notwendige Netztrennung aufgehoben werden. Unter Umständen können hierdurch virtuelle Clients unerlaubt miteinander kommunizieren.

Diese Situation ergibt sich beispielsweise, wenn die virtuellen Clients den Benutzenden auf Basis von Eigenschaften wie Gruppenzugehörigkeiten zugewiesen und falsch zugeordnet werden. In diesem Fall kann eine Netztrennung umgangen werden, die eigentlich zwischen Clients verschiedener Gruppen bestehen sollte.

2.4. Verlust von virtuellen Clients durch Fehlkonfiguration in der VDI

Eine Stärke von VDI ist es, dass viele verschiedene virtuelle Clients über wenige Vorlagen (Templates) einfach verwaltet werden können. Damit können neue Desktops schnell provisioniert sowie fehlerhafte Desktops repariert oder ausgetauscht werden.

Durch diese zentralisierte Verwaltung können aber durch gelöschte oder korrumpierte Templates virtuelle Clients verloren gehen. Werden bestimmte Daten von Benutzenden ausschließlich auf dem Speicher der virtuellen Clients abgelegt, führt der Verlust eines virtuellen Clients auch zu einem Verlust dieser Daten.

Auch von den Benutzenden geänderte Konfigurationen werden unwiederbringlich gelöscht, wenn der virtuelle Client zurückgesetzt wird.

2.5. Ausfall von VDI-Komponenten

Eine VDI besteht typischerweise aus mehreren Komponenten, die voneinander abhängen. Fällt auch nur eine dieser Komponenten aus, beispielsweise aufgrund von Hard- oder Software-Fehlern oder aufgrund von Fehlkonfigurationen, kann dies die Verfügbarkeit der gesamten VDI-Lösung und damit die Arbeitsfähigkeit der Benutzenden beeinträchtigen.

Ein Ausfall einer oder mehrerer Komponenten kann sehr unterschiedliche Auswirkungen haben. Beispielsweise ist beim Ausfall der VDI-Managementkomponente prinzipiell ein normaler Arbeitsbetrieb möglich, aber es können keine Anpassungen vorgenommen werden. Dies kann unter anderem dazu führen, dass

- neue virtuelle Clients nicht bereitgestellt werden können,
- virtuelle Clients nach Fehlern nicht in einen funktionsfähigen Basiszustand zurückgesetzt werden können,
- das Troubleshooting erschwert wird, da die gesammelten Informationen der Managementfunktionen nicht verfügbar sind oder
- die Ressourcen eines virtuellen Clients nicht angepasst werden können, falls diese für Einzelne nicht ausreichen.

Die Zugangs- oder Steuerungskomponenten mancher VDI-Produkte bieten ohne die Managementkomponente nicht ihren vollen Funktionsumfang.

2.6. Unberechtigter Zugriff auf virtuelle Clients

Eine VDI-Managementkomponente verwaltet alle zugehörigen Clients. Wird die VDI-Managementkomponente kompromittiert (beispielsweise aufgrund ausgenutzter Schwachstellen oder Fehlkonfiguration), kann von dort aus auf die virtuellen Clients zugegriffen werden. In diesem Fall können Verfügbarkeit, Vertraulichkeit oder Integrität der virtuellen Clients beeinträchtigt werden.

Einige VDI-Lösungen bringen eine Agentensoftware mit sich, die innerhalb der virtuellen Clients genutzt und für bestimmte VDI-Funktionen (z. B. Verbindungsaufbau, 3D-Beschleunigung, Optimierung des Speicherverbrauchs) benötigt wird. Wirkt sich eine Fehlkonfiguration auf diese Agentensoftware aus, können die virtuellen Clients gefährdet sein.

Die Agentensoftware und die Managementkomponente der VDI steuern je nach Größe der Umgebung viele Clients. In diesen Fällen kann auf viele verschiedene virtuelle Clients zugegriffen werden.

2.7. Nutzung von Templates mit Software-Schwachstellen

In einer VDI können schnell und zentralisiert virtuelle Clients aus einer definierten Menge von Templates erzeugt werden. Wenn diese Templates erzeugt werden, sind sie in der Regel auf einem aktuellen Software-Stand ohne bekannte Schwachstellen.

Ohne eine regelmäßige Aktualisierung dieser Templates ist es jedoch möglich, dass ein neu erzeugter virtueller Client Schwachstellen aufweist, die bekannt wurden, nachdem das Template erzeugt wurde. Können andere IT-Systeme auf diesen virtuellen Client zugreifen, kann die bekannte Schwachstelle ausgenutzt werden und somit der virtuelle Client kompromittiert werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.2.6 *Virtual Desktop Infrastructure* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Planende

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.2.6.A1 Planung des Einsatzes einer VDI (B)

Die Leistungsanforderungen und Anzahl der benötigten virtuellen Clients sowie die daraus resultierenden Anforderungen an die Dimensionierung der VDI MÜSSEN identifiziert werden. Die VDI-Komponenten MÜSSEN anhand dieser Dimensionierungsanforderungen bedarfsgerecht geplant werden. Die VDI-Komponenten und die genutzte Virtualisierungsinfrastruktur MÜSSEN aufeinander abgestimmt geplant werden.

Bei der Dimensionierung der VDI MUSS berücksichtigt werden, ob und wie sich die Anforderungen hieran über den geplanten Einsatzzeitraum der VDI-Lösung ändern. Der Support MUSS für den gesamten geplanten Einsatzzeitraum der VDI-Lösung bei der Planung mitberücksichtig werden.

Die Anzahl virtueller Clients und deren benötigte Leistung pro Virtualisierungsserver MUSS festgelegt werden.

SYS.2.6.A2 Sichere Installation und Konfiguration der VDI-Komponenten (B)

Wenn die VDI-Komponenten installiert und konfiguriert werden, MUSS mindestens berücksichtigt werden, wie:

- auf betrieblich und technisch notwendige Funktionen beschränkt wird,
- die Kommunikation zwischen VDI-Komponenten abgesichert wird sowie
- virtuelle Clients sicher den Benutzenden oder Gruppen hiervon zugewiesen werden.

Empfehlungen von dem herstellenden Unternehmen der VDI-Lösung für die sichere Konfiguration MÜSSEN berücksichtigt werden.

Die Konfigurationen der VDI-Komponenten MÜSSEN geeignet dokumentiert werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.2.6.A3 Sichere Installation und Konfiguration der virtuellen Clients mithilfe der VDI (S)

Die VDI-Lösung SOLLTE genutzt werden, um die virtuellen Clients zu installieren und zu konfigurieren. Virtuelle Clients SOLLTEN NICHT manuell in die VDI-Lösung integriert werden. In der für die VDI verwendeten Virtualisierungsinfrastruktur SOLLTEN virtuelle Clients NICHT unabhängig von der VDI erzeugt werden.

SYS.2.6.A4 Netzsegmentierung der VDI-Komponenten (S) [Planende]

Die VDI-Komponenten inklusive der virtuellen Clients SOLLTEN bei der Netzsegmentierung gesondert berücksichtigt werden. Netze SOLLTEN dabei mindestens mit Hilfe der Virtualisierungsinfrastruktur getrennt werden. Dedizierte Netzsegmente SOLLTEN mindestens für das Administrationsnetz der VDI-Komponenten und für die Netze der internen Kommunikation zwischen VDI-Komponenten eingerichtet werden.

SYS.2.6.A5 Standardisierter Zugriff auf virtuelle Clients (S)

Die Mechanismen und Dienste der VDI-Lösung SOLLTEN genutzt werden, um die Zugriffe auf die virtuellen Clients zu steuern und abzusichern. Falls eine zusätzliche Software für diese Zugriffe auf den zugreifenden Clients eingesetzt wird, SOLLTE diese Software standardisiert und zentralisiert bereitgestellt werden.

SYS.2.6.A6 Verwendung einer dedizierten Infrastruktur für virtuelle VDI-Komponenten (S)

Falls die VDI-Komponenten virtualisiert betrieben werden, SOLLTEN sie auf einer dedizierten Virtualisierungsinfrastruktur betrieben werden.

SYS.2.6.A7 Härtung der virtualisierten Clients durch die VDI-Lösung (S)

Die Möglichkeiten der VDI-Lösung SOLLTEN für die Härtung der virtuellen Clients entsprechend den Anforderungen des Bausteins SYS.2.5 *Client-Virtualisierung* genutzt werden. Die Betriebssysteme der Clients SOLLTEN ausschließlich über die Managementkomponente der VDI-Lösung konfiguriert werden. Eine individuelle Konfiguration bestehender virtueller Clients über die Virtualisierungsinfrastruktur SOLLTE mit technischen Mitteln unterbunden werden.

SYS.2.6.A8 Härtung der VDI-Lösung (S)

Eine automatische Anmeldung an der VDI SOLLTE nicht möglich sein. Die Authentisierung SOLLTE nur erfolgen, nachdem die Benutzenden mit der VDI interagiert haben.

SYS.2.6.A9 Einbindung der virtuellen Clients in das Patch- und Änderungsmanagement (S)

Die virtuellen Clients SOLLTEN, wenn möglich, zentral über die Managementkomponenten der VDI-Lösung verwaltet werden. Die virtuellen Clients SOLLTEN auch im ausgeschalteten Zustand gepatcht werden, falls dies von der VDI-Lösung unterstützt wird. Die Templates, aus denen virtuelle Clients erzeugt werden, SOLLTEN regelmäßig aktualisiert werden.

SYS.2.6.A10 Monitoring von Verfügbarkeit und Nutzungsgrad der VDI (S)

Der Zustand der VDI-Komponenten SOLLTE zentral überwacht werden. Es SOLLTEN mindestens folgende Parameter für jede VDI-Komponente überwacht werden:

- Erreichbarkeit der benötigten Netzschnittstellen
- Verfügbarkeit der von der VDI-Komponente bereitgestellten Dienste
- Auslastung der CPU und des Arbeitsspeichers

SYS.2.6.A11 Monitoring von sicherheitsrelevanten Ereignissen der VDI (S)

Für die VDI-Komponenten SOLLTEN mindestens die folgenden Ereignisse an ein zentrales Monitoring weitergeleitet werden:

- erfolgreiche und fehlgeschlagene Anmeldeversuche
- Konfigurationsänderungen an VDI-Komponenten oder virtuellen Clients
- erfolgreiche und fehlgeschlagene Updates an VDI-Komponenten
- fehlgeschlagene Updates an virtuellen Clients

Die VDI-Komponenten SOLLTEN regelmäßig auf Schwachstellen überprüft werden.

SYS.2.6.A12 Verteilung von virtuellen Clients auf Virtualisierungsservern (S)

Pro Virtualisierungsserver SOLLTE die maximale Leistung festgelegt werden, die dieser für virtuelle Clients zur Verfügung stellen darf. Diese Grenzwerte SOLLTEN in der VDI-Managementkomponente genutzt werden, um bei hoher Auslastung die virtuellen Clients auf verschiedene Virtualisierungsserver zu verteilen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.2.6.A13 Verwendung getrennter VDI-Lösungen für unterschiedliche Benutzendengruppen (H)

Es SOLLTE geprüft werden, ob es Benutzendengruppen gibt, die sich in ihren Berechtigungen so stark unterscheiden, dass die Nutzung einer gemeinsamen VDI-Lösung nicht sinnvoll ist. In diesem Fall SOLLTE jeweils eine eigene VDI-Lösung pro Benutzendengruppe verwendet werden.

SYS.2.6.A14 Verwendung von nicht-persistenten virtuellen Clients (H)

Nachdem sie benutzt wurden oder zu einem definierten Zeitpunkt SOLLTEN die virtuellen Clients auf ihren Grundzustand, d. h. auf das zugrundeliegende Template, zurückgesetzt oder bei Bedarf neu provisioniert werden. Diese Zeitfenster SOLLTEN dokumentiert und an die Betroffenen kommuniziert werden. Nicht zurückgesetzte virtuelle Clients SOLLTEN NICHT von mehreren unterschiedlichen Benutzenden verwendet werden.

SYS.2.6.A15 Hochverfügbare Bereitstellung der VDI-Komponenten (H)

Die VDI-Komponenten SOLLTEN redundant ausgelegt werden. Jede Komponente SOLLTE darüber hinaus redundant an die relevanten Netze angeschlossen werden. Falls die VDI-Komponenten auf physischen IT-Systemen betrieben werden, SOLLTEN diese IT-Systeme über redundante Stromversorgung und Datenspeicher verfügen. Falls die VDI-Komponenten virtualisiert betrieben werden, SOLLTEN Mechanismen der Virtualisierungsinfrastruktur für die Hochverfügbarkeit eingesetzt werden.

SYS.2.6.A16 Integration der VDI in ein SIEM (H)

Wird ein Security Information and Event Management (SIEM) genutzt, SOLLTEN die VDI-Komponenten darin eingebunden werden. Im SIEM SOLLTEN die überwachten Ereignisse automatisiert hinsichtlich Anomalien inklusive Angriffsmustern analysiert werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein SYS.2.6 *Virtual Desktop Infrastructure* sind keine weiterführenden Informationen vorhanden.

Bundesamt
für Sicherheit in der
Informationstechnik

SYS.3.1 Laptops

1. Beschreibung

1.1. Einleitung

Ein Laptop (auch Notebook genannt) ist ein PC, der mobil genutzt werden kann. Er hat eine kompakte Bauform, integriert Peripheriegeräte wie Tastatur und Bildschirm, ist über Akkus zeitweise unabhängig von einer externen Stromversorgung und besteht oft aus speziell für den mobilen Einsatz konzipierten Hardware-Komponenten. Laptops sind in den meisten Institutionen verbreitet und ersetzen häufig den klassischen Desktop-PC.

Laptops werden in der Regel mit verbreiteten Desktop-Betriebssystemen wie Microsoft Windows, Apple macOS oder Linux betrieben. Die Grenzen zu Tablets und ähnlichen Geräten sind heutzutage fließend. So gibt es Tablets mit Desktop-Betriebssystemen wie Windows 10, aber auch Tastaturzubehör für Mobilgeräte wie iPads mit iPadOS, die so als Laptops genutzt werden können.

Da Laptops häufig auch mobil genutzt werden, sind sie oft nicht permanent am LAN der Institution angeschlossen. Stattdessen können sie sich in der Regel per Virtual Private Network (VPN) z. B. über das Internet mit dem Netz der Institution verbinden. Auch die Infrastruktur einer klassischen Büroumgebung, die kontrollierbare Umwelteinflüsse, eine stabile Stromversorgung oder zutrittsgeschützte Bereiche bietet, kann beim mobilen Einsatz von Laptops nicht vorausgesetzt werden.

1.2. Zielsetzung

Ziel des Bausteins ist es, Institutionen einen sicheren Einsatz von Laptops zu ermöglichen sowie für die spezifischen Gefährdungen dieser Geräteklasse zu sensibilisieren.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.3.1 *Laptops* ist auf alle Laptops anzuwenden, die mobil oder stationär genutzt werden.

Wie bei allen IT-Systemen müssen auch bei Laptops die Betriebssystem- und Software-Komponenten sorgfältig ausgewählt und installiert werden. Die hier zu erfüllenden Anforderungen sind abhängig vom Betriebssystem des Laptops und werden daher in den Client-spezifischen Bausteinen beschrieben, beispielsweise SYS.2.2.3 *Clients unter Windows,* SYS 2.3 *Clients unter Linux und Unix* oder SYS.2.4 *Clients unter macOS*. Ebenso sind Anforderungen, die für alle Arten von Clients gelten, nicht Bestandteil dieses Bausteins. Diese sind im Baustein SYS.2.1 *Allgemeiner Client* zu finden.

Auch wird in diesem Baustein nicht behandelt, wie die jeweilige Datenübertragung einzurichten ist, wie z. B. die WLAN-Konfiguration (siehe NET.2.2 *WLAN-Nutzung*) oder eine VPN-Anbindung (siehe NET.3.3 *VPN*).

Da Laptops oft längere Zeit außerhalb einer Institution eingesetzt werden, müssen sie besonders bei der Datensicherung berücksichtigt werden. Weiterführende Anforderungen dazu finden sich in Baustein CON.3 *Datensicherungskonzept*.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein *SYS.3.1 Laptops* von besonderer Bedeutung.

2.1. Beeinträchtigung durch wechselnde Einsatzumgebung

Laptops werden in sehr unterschiedlichen Umgebungen eingesetzt und sind dadurch vielen Gefährdungen ausgesetzt. Dazu gehören beispielsweise schädigende Umwelteinflüsse wie zu hohe oder zu niedrige Temperaturen, ebenso Staub oder Feuchtigkeit. Bei Laptops besteht auch stets die Gefahr von Transportschäden. Außerdem kommunizieren Laptops vor allem unterwegs oft mit unbekannten IT-Systemen oder Netzen, was immer ein Gefährdungspotenzial für das eigene Gerät mit sich bringt. So können dabei beispielsweise Schadprogramme übertragen oder schützenswerte Informationen kopiert werden.

2.2. Diebstahl und Verlust von Laptops

Mitarbeitende nutzen ihre Laptops oftmals auch außerhalb der Institution. Die Geräte werden etwa in privaten Kraftfahrzeugen oder in öffentlichen Verkehrsmitteln transportiert, in fremden Büroräumen in Pausen zurückgelassen oder in Hotelzimmern unbewacht aufgestellt. Somit sind Laptops einem höheren Diebstahlrisiko ausgesetzt und können zudem leicht vergessen oder verloren werden. Kommt ein Laptop abhanden, entstehen Kosten und Aufwand für die Wiederbeschaffung. Nicht gesicherte Daten sind zudem verloren. Ebenso könnten Unbefugte auf schützenswerte Daten zugreifen, wodurch es zu weiteren Schäden kommen kann. Diese wiegen in vielen Fällen deutlich schwerer als der rein materielle Verlust des Laptops.

2.3. Ungeordnete Weitergabe von Laptops

Wenn Mitarbeitende nur in Ausnahmefällen mobile IT-Systeme benötigen, wie beispielsweise für selten durchgeführte Dienstreisen, ist es oft zweckmäßiger, nur wenige Laptops zentral vorzuhalten. Diese können dann untereinander weitergereicht werden. Wird jedoch der Laptop einfach an den nächsten Mitarbeitenden übergeben, besteht die Gefahr, dass noch auf dem Gerät befindliche schutzbedürftige Daten weitergegeben werden. Außerdem ist es möglich, dass der Laptop mit Schadsoftware infiziert ist. Ohne eine geeignete Regelung kann schwer nachvollziehbar sein, wer den Laptop wann benutzt hat oder wer ihn zurzeit benutzt.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.3.1 *Laptops* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzende, Beschaffungsstelle

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.3.1.A1 Regelungen zur mobilen Nutzung von Laptops (B)

Es MUSS klar geregelt werden, was Mitarbeitende bei der mobilen Nutzung von Laptops berücksichtigen müssen. Es MUSS insbesondere festgelegt werden, welche Laptops mobil genutzt werden dürfen, wer sie mitnehmen darf und welche grundlegenden Sicherheitsmaßnahmen dabei zu beachten sind. Die Benutzenden MÜSSEN auf die Regelungen hingewiesen werden.

SYS.3.1.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.3.1.A3 Einsatz von Personal Firewalls (B)

Auf Laptops MUSS eine Personal Firewall aktiv sein, wenn sie außerhalb von Netzen der Institution eingesetzt werden. Die Filterregeln der Firewall MÜSSEN so restriktiv wie möglich sein. Die Filterregeln MÜSSEN regelmäßig getestet werden. Die Personal Firewall MUSS so konfiguriert werden, dass die Benutzenden nicht durch Warnmeldungen belästigt werden, die sie nicht interpretieren können.

SYS.3.1.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.3.1.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.3.1.A9 Sicherer Fernzugriff mit Laptops (B)

Aus öffentlich zugänglichen Netzen DARF NUR über einen sicheren Kommunikationskanal auf das interne Netz der Institution zugegriffen werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.3.1.A6 Sicherheitsrichtlinien für Laptops (S)

Für Laptops SOLLTE eine Sicherheitsrichtlinie erstellt werden, die regelt, wie die Geräte benutzt werden dürfen. Die Benutzenden SOLLTEN hinsichtlich des Schutzbedarfs von Laptops und der dort gespeicherten Daten sensibilisiert werden. Auch SOLLTEN sie auf die spezifischen Gefährdungen bzw. die entsprechenden Anforderungen für die Nutzung aufmerksam gemacht werden. Sie SOLLTEN außerdem darüber informiert werden, welche Art von Informationen sie auf Laptops verarbeiten dürfen.

SYS.3.1.A7 Geregelte Übergabe und Rücknahme eines Laptops (S) [Benutzende]

Wenn Laptops von verschiedenen Personen abwechselnd genutzt werden, SOLLTE geregelt werden, wie sie sicher übergeben werden können. Auch SOLLTE geregelt werden, wie sie wieder sicher zurückzunehmen sind. Vor der Weitergabe eines Laptops SOLLTEN eventuell vorhandene schützenswerte Daten sicher gelöscht werden. Falls der Laptop vor der Weitergabe nicht neu aufgesetzt wird, SOLLTE sichergestellt sein, dass sich auf dem IT-System und allen damit verbundenen Datenträgern keine Schadsoftware befindet. Gemeinsam mit einem Laptop SOLLTE ein Merkblatt für den sicheren Umgang mit dem Gerät ausgehändigt werden.

SYS.3.1.A8 Sicherer Anschluss von Laptops an Datennetze (S) [Benutzende]

Es SOLLTE geregelt werden, wie Laptops sicher an eigene oder fremde Datennetze und an das Internet angeschlossen werden. Nur zugelassene Laptops SOLLTEN sich am internen Netz der Institution anmelden können.

SYS.3.1.A10 Abgleich der Datenbestände von Laptops (S) [Benutzende]

Es SOLLTE geregelt werden, wie Daten von Laptops in den Informationsverbund der Institution übernommen werden. Wenn ein Synchronisationstool benutzt wird, SOLLTE sichergestellt sein, dass Synchronisationskonflikte aufgelöst werden können. Der Synchronisationsvorgang SOLLTE protokolliert werden. Außerdem SOLLTEN die Benutzenden angewiesen werden, die Synchronisationsprotokolle zu prüfen.

SYS.3.1.A11 Sicherstellung der Energieversorgung von Laptops (S) [Benutzende]

Alle Benutzenden SOLLTEN darüber informiert werden, wie sie die Energieversorgung von Laptops im mobilen Einsatz optimal sicherstellen können. Vorhandene Ersatzakkus SOLLTEN in geeigneten Hüllen gelagert und transportiert werden.

SYS.3.1.A12 Verlustmeldung für Laptops (S) [Benutzende]

Benutzende SOLLTEN umgehend melden, wenn ein Laptop verloren gegangen ist oder gestohlen wurde. Dafür SOLLTE es in der Institution klare Meldewege geben. Wenn verlorene Laptops wieder auftauchen, SOLLTE untersucht werden, ob sie eventuell manipuliert wurden. Die darauf eingesetzte Software inklusive des Betriebssystems SOLLTE komplett neu installiert werden.

SYS.3.1.A13 Verschlüsselung von Laptops (S)

In Laptops verbaute Datenträger wie Festplatten oder SSDs SOLLTEN verschlüsselt werden.

SYS.3.1.A14 Geeignete Aufbewahrung von Laptops (S) [Benutzende]

Alle Benutzenden SOLLTEN darauf hingewiesen werden, wie Laptops außerhalb der Institution sicher aufzubewahren sind. Abhängig vom Schutzbedarf der darauf gespeicherten Daten SOLLTEN Laptops auch in den Räumen der Institution außerhalb der Nutzungszeiten gegen Diebstahl gesichert bzw. verschlossen aufbewahrt werden.

SYS.3.1.A15 Geeignete Auswahl von Laptops (S) [Beschaffungsstelle]

Bevor Laptops beschafft werden, SOLLTE eine Anforderungsanalyse durchgeführt werden. Anhand der Ergebnisse SOLLTEN alle infrage kommenden Geräte bewertet werden. Die Beschaffungsentscheidung SOLLTE mit dem IT-Betrieb abgestimmt sein.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.3.1.A16 Zentrale Administration und Verwaltung von Laptops (H)

Es SOLLTE eine geeignete Regelung definiert werden, wie Laptops zentral zu administrieren und verwalten sind. Ein Tool zum zentralen Laptop-Management SOLLTE möglichst alle eingesetzten Betriebssysteme unterstützen.

SYS.3.1.A17 Sammelaufbewahrung von Laptops (H)

Nicht benutzte Laptops SOLLTEN in einem geeignet abgesicherten Raum vorgehalten werden. Der dafür genutzte Raum SOLLTE den Anforderungen aus dem Baustein INF.5 *Raum sowie Schrank für technische Infrastruktur* entsprechen.

SYS.3.1.A18 Einsatz von Diebstahl-Sicherungen (H)

Es SOLLTE geregelt werden, welche Diebstahlsicherungen für Laptops eingesetzt werden sollen. Bei mechanischen Sicherungen SOLLTE besonders auf ein gutes Schloss geachtet werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein SYS.3.1 *Laptops* sind keine weiterführenden Informationen vorhanden.

Bundesamt
für Sicherheit in der
Informationstechnik

SYS.3.2.1 Allgemeine Smartphones und Tablets

1. Beschreibung

1.1. Einleitung

Smartphones sind auf den mobilen Einsatz ausgerichtete IT-Systeme mit einer angepassten Oberfläche, die mit einem großen, üblicherweise berührungsempfindlichen Bildschirm (Touch-Display) bedient werden können. Smartphones vereinen neben der Telefonie beispielsweise Media-Player, Personal Information Manager und Digitalkamera in einem Gerät und bieten den Benutzenden darüber hinaus viele weitere Anwendungen und Funktionen, wie Webbrowser, E-Mail-Client oder Ortung (z. B. über GPS). Zudem sind sie mit Mobilfunk-, WLAN-, Bluetooth- sowie NFC-Schnittstellen ausgestattet. Tablets sind, vereinfacht gesagt, Smartphones mit großem Formfaktor, mit denen in der Regel nicht über das Mobilfunknetz telefoniert werden kann.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, den Zuständigen des Sicherheitsmanagements und des IT-Betriebs Informationen zu den typischen Gefährdungen für Smartphones und Tablets zu geben sowie ihnen Anforderungen zu vermitteln, wie diese vermieden bzw. beseitigt werden können. Außerdem sollen den Zuständigen Ansätze aufgezeigt werden, um schutzbedarfsgerechte Konfigurationsprofile zu erstellen. Diese Konfigurationsprofile können über eine zentrale Infrastruktur mit einem Mobile Device Management (MDM) verteilt und verwaltet werden. Es kann jedoch bei der Vielzahl von unterschiedlichen mobilen Betriebssystemen nicht grundsätzlich vorausgesetzt werden, dass die Geräte in ein solches MDM eingebunden werden können.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets* ist für alle Smartphones und Tablets anzuwenden, die für dienstliche Zwecke eingesetzt werden.

Dieser Baustein geht nicht darauf ein, wie spezifische Betriebssysteme von Smartphones und Tablets abgesichert werden, da dies detailliert in den Bausteinen für die jeweiligen Systeme beschrieben wird, z. B. in SYS.3.2.3 *iOS (for Enterprise)* oder SYS.3.2.4 *Android*. Sicherheitsanforderungen für den Betrieb eines MDM werden in SYS.3.2.2 *Mobile Device Management (MDM)* beschrieben. Diese Bausteine sind entsprechend zusätzlich anzuwenden, wenn Smartphones und Tablets in Institutionen eingesetzt werden.

Smartphones sind, so wie gewöhnliche Clients, durch Schadprogramme gefährdet. Sie müssen im Konzept zum Schutz vor Schadsoftware berücksichtigt werden. Anforderungen zum Schutz vor Schadprogrammen finden sich im Baustein OPS.1.1.4 *Schutz vor Schadprogrammen*.

Smartphones und Tablets bieten in der Regel die Möglichkeit, mobile Anwendungen (Apps) zu installieren. Damit dabei keine unnötigen Sicherheitsrisiken entstehen, sind die Anforderungen des Bausteins APP.1.4 *Mobile Anwendungen (Apps)* zu berücksichtigen. Darüber hinaus können aus der Schicht APP *Anwendungen* auch andere Bausteine, wie APP.1.2 *Webbrowser,* relevant sein.

Da Smartphones in der Regel über Mobilfunkfunktionen verfügen, sind die relevanten Anforderungen des Bausteins SYS.3.3 *Mobiltelefon* zu berücksichtigen.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets* von besonderer Bedeutung.

2.1. Fehlende Betriebssystem-Updates

Es erscheinen regelmäßig neue Versionen und Updates von mobilen Betriebssystemen. Diese müssen bei Geräten, die spezifische Erweiterungen des Betriebssystems der herstellenden Institution haben, erst von diesen in ihre Version integriert und anschließend verteilt werden. Updates werden in der Regel für die neueste Gerätegeneration und für eine Reihe von älteren Gerätegenerationen bereitgestellt. Allerdings werden nicht alle zurückliegenden Betriebssystem-Versionen im gleichen Umfang mit (Sicherheits-) Updates versorgt. Teilweise werden Betriebssysteme auch aus wirtschaftlichen Gründen nicht weiterentwickelt. Nachträglich bekannt gewordene Schwachstellen im Betriebssystem einer bereits abgekündigten Gerätegeneration können dann nicht mehr durch Updates geschlossen und bei einem Angriff besonders leicht ausgenutzt werden.

2.2. Software-Schwachstellen in vorinstallierten Anwendungen (Apps)

Auch bereits vorinstallierte Apps können Schwachstellen enthalten, die für lokale Angriffe oder für Angriffe über Netzverbindungen ausgenutzt werden können. Außerdem werden viele Apps von Drittentwickelnden nach einiger Zeit nicht mehr weiter gepflegt. Folglich können erkannte Sicherheitsmängel dann nicht mehr durch entsprechende Updates behoben werden.

2.3. Manipulation von Smartphones und Tablets

Bei einem Angriff kann sich Zugang zu Smartphones oder Tablets verschafft werden, um gezielt Daten zu manipulieren. So könnte beispielsweise die Konfiguration geändert, zusätzliche Dienste gestartet oder Schadsoftware installiert werden. Dadurch kann auf dem manipulierten System beispielsweise die Kommunikationsverbindungen mitgeschnitten (ungewollter Datenabfluss) oder Sicherheitseinstellungen verändert werden (z. B. Zugriffe aus dem Internet auf das Endgerät erlauben).

2.4. Schadprogramme für Smartphones und Tablets

Wie jedes mit dem Internet verbundene Gerät sind auch mobile Endgeräte von Schadsoftware bedroht. Das Infektionsrisiko ist, verglichen mit Client-Betriebssystemen wie Microsoft Windows, zwar noch geringer, jedoch konzentrieren sich Angreifende immer mehr auf mobile Geräte. Insbesondere wenn Apps aus nicht vertrauenswürdigen Quellen bezogen werden oder keine Updates für bekannte Schwachstellen verfügbar sind, besteht die Gefahr einer Infektion. Wird ein Gerät infiziert, können beispielsweise Daten ausgelesen, verändert, gelöscht oder auf interne IT-Ressourcen der Institution zugegriffen oder im Namen der Institution agiert werden.

2.5. Webbasierte Angriffe auf mobile Browser

Mobile Browser, aber auch viele andere Apps, können Webseiten und Webinhalte anzeigen. Dadurch können die Geräte von Phishing-Angriffen, Drive-by-Exploits und anderen webbasierten Angriffsformen betroffen sein.

2.6. Missbrauch von Gesundheits-, Fitness- und Ortungsdaten

Das Betriebssystem vieler Smartphones und Tablets enthält meist spezielle Funktionen, um Gesundheits-, Fitness- und Ortungsdaten zu verwalten. Diese personenbezogenen Daten stellen ein attraktives Angriffsziel dar und sind besonders schützenswert, insbesondere wenn sie über einen längeren Zeitraum gesammelt und gespeichert werden. Voraussetzung ist, dass diese Funktionen aktiviert wurden.

So kann z. B. der Standort des Gerätes durch einen Angriff auf das Gerät selbst oder auf damit verbundene Cloud-Dienste erkennbar sein. Das kann neben den datenschutzrechtlichen Auswirkungen unter Umständen auch zu weiteren Angriffen führen. So sind beispielsweise Einbrüche bei Mitarbeitenden denkbar, die sich laut Standort auf Reisen befinden.

2.7. Missbrauch schutzbedürftiger Daten im Sperrbildschirm

Viele mobile Betriebssysteme verfügen über eine Funktion, die es ermöglicht, Mitteilungen von aktivierten Widgets und Push-Nachrichten auf dem Sperrbildschirm anzeigen zu lassen. Hierdurch können vertrauliche Informationen unberechtigten Dritten preisgegeben und durch diese ausgenutzt werden. Über Sprachassistenten besteht zudem oft auch im gesperrten Zustand die Möglichkeit, auf Telefonfunktionen und Kontaktdaten zuzugreifen. Auch dies kann dazu führen, dass unberechtigte Dritte an vertrauliche Informationen gelangen können.

Zudem besteht im gesperrten Zustand oft die Möglichkeit, Schnittstellen wie WLAN oder Bluetooth zu konfigurieren. So lässt sich beispielsweise ein zusätzlicher Angriffsvektor aktivieren, wenn die Bluetooth-Schnittstelle durch einen Angreifenden mit physischem Zugriff eingeschaltet wird.

2.8. Gefahren durch private Nutzung dienstlicher Smartphones und Tablets

Wenn Mitarbeitende firmeneigene Smartphones und Tablets privat benutzen, entstehen gleich mehrere Probleme für die Informationssicherheit der Institution. So könnten die Benutzenden etwa selbstständig Apps installieren, die Schadfunktionen enthalten, oder sie besuchen eine Webseite, die das Gerät mit Malware infiziert. Ebenso sind viele privat installierte Apps ein Risiko für die auf dem Gerät gespeicherten Informationen der Institution, da sie z. B. Adressbücher auslesen und zu unbekannten Servern übertragen oder möglicherweise auf E-Mails oder Dokumente zugreifen können. So könnten Daten abfließen oder umgekehrt unkontrolliert in die Institution gelangen. Typische Beispiele für Apps mit solchen Risiken sind Social-Media- und Messenger-Apps.

2.9. Gefahren durch Bring Your Own Device (BYOD)

Werden private Endgeräte dienstlich genutzt, ergeben sich dadurch verschiedene Gefährdungspotentiale. Beispielsweise können bezüglich der Software-Lizenzen rechtliche Probleme eintreten. Wenn im Notfall dienstliche Daten durch das MDM auf dem Gerät gelöscht werden müssen, kann dies auch Auswirkungen auf die privaten Daten auf dem Gerät haben.

Zudem können die IT-Zuständigen nicht jedes einzelne private Gerät daraufhin prüfen, ob es den dienstlichen Anforderungen genügt. Dadurch können Geräte verwendet werden, mit denen die Benutzenden gegen Datenschutz- und Sicherheitsanforderungen verstoßen. Zudem sind die Benutzenden oft selbst dafür zuständig, ihre Geräte zu warten und reparieren zu lassen. Bei einer solchen Reparatur könnten beispielsweise Firmendaten unbefugt eingesehen werden. Die gleiche Gefahr besteht, falls nicht geregelt ist, was mit den Daten auf dem Gerät geschehen soll, wenn Mitarbeitende aus der Institution ausscheiden.

2.10. Rechteerhöhung durch Schwachstellen

In Betriebssysteme von Smartphones und Tablets werden immer wieder Schwachstellen entdeckt, die es ermöglichten, das von den herstellenden Institutionen etablierte Sicherheitskonzepte zu umgehen und somit auf Systemprozesse und geschützte Speicherbereiche zuzugreifen. Dadurch können Programme nicht vorgesehene Berechtigungen erlangen, mit denen sie unerlaubte Aktionen ausführen können. Beispielsweise könnten die Programme so auf Daten des Betriebssystems und anderer Apps zugreifen.

Sogenannte Jailbreaks nutzen diese Schwachstellen aus, um beispielsweise alternative App-Stores oder sonstige Erweiterungen nutzen zu können. Jailbreak-Techniken können im Falle eines Angriffs dafür verwendet werden, um Schadprogramme zu installieren oder andere schädliche Manipulationen auf dem Gerät vorzunehmen.

Schadprogramme können auch Schwachstellen ausnutzen, um sich auf einem Gerät zu installieren oder es zu manipulieren. Hierdurch kann das Betriebssystem anders als vorgesehen genutzt und wichtige Sicherheitsfunktionen können übergangen werden.

Insbesondere betroffen sind Daten, die vom mobilen Betriebssystem in geschützten Bereichen gelagert werden, da eine App mit Superuser-Rechten diese unter Umständen auslesen kann.

Durch beabsichtigte Rechteerhöhung („Rooten") können ähnliche Gefährdungsszenarien entstehen, wenn der Zugriff auf die privilegierten Rechte nicht geschützt wird.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.3.2.1 *Allgemeine Smartphones und Tablets* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzende

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.3.2.1.A1 Festlegung einer Richtlinie für den Einsatz von Smartphones und Tablets (B)

Bevor eine Institution Smartphones oder Tablets bereitstellt, betreibt oder einsetzt, MUSS eine generelle Richtlinie für die Nutzung und Kontrolle der Geräte festgelegt werden. Hierbei MUSS unter anderem festgelegt werden, wer mit Smartphones auf welche Informationen der Institution zugreifen darf.

SYS.3.2.1.A2 Festlegung einer Strategie für die Cloud-Nutzung (B)

Die Institution MUSS im Zusammenhang mit Smartphones und Tablets eine generelle Strategie für die Cloud-Nutzung sowie für den Schutz und die Kontrolle der Informationen festlegen. Die erlaubte Nutzung von Cloud-Diensten für Informationen der Institution MUSS geklärt und festgelegt werden. Es MUSS festgelegt werden, ob und in welchem Umfang Cloud-Dienste bei privater Nutzung der Geräte erlaubt sind. Die Benutzenden MÜSSEN regelmäßig bezüglich der Nutzung solcher Cloud-Dienste sensibilisiert werden.

SYS.3.2.1.A3 Sichere Grundkonfiguration für mobile Geräte (B)

Alle mobilen Endgeräte MÜSSEN so konfiguriert sein, dass sie das erforderliche Schutzniveau angemessen erfüllen. Dafür MUSS eine passende Grundkonfiguration der Sicherheitsmechanismen und -einstellungen zusammengestellt und dokumentiert werden. Nicht benötigte Funktionen SOLLTEN deaktiviert werden. Die Freischaltung von Kommunikationsschnittstellen MUSS geregelt und auf das dienstlich notwendige Maß reduziert werden. Nicht benutzte Schnittstellen SOLLTEN deaktiviert werden.

SYS.3.2.1.A4 Verwendung eines Zugriffsschutzes (B) [Benutzende]

Smartphones und Tablets MÜSSEN mit einem angemessen komplexen Gerätesperrcode geschützt werden. Die Bildschirmsperre MUSS genutzt werden. Die Anzeige von vertraulichen Informationen auf dem Sperrbildschirm MUSS deaktiviert sein. Alle mobilen Geräte MÜSSEN nach einer angemessen kurzen Zeitspanne selbsttätig die Bildschirmsperre aktivieren. Diese Zeitspanne MUSS in Abhängigkeit zum angestrebten Schutzniveau stehen.

Bei jedem fehlgeschlagenen Versuch, das Gerät zu entsperren, SOLLTE sich die Wartezeit zu einem neuen Versuch verlängern. Die Anzahl der Gerätesperrcodes, nach der sich ein Code wiederholen darf, SOLLTE festgelegt werden. Nach mehreren fehlgeschlagenen Versuchen, den Bildschirm zu entsperren, SOLLTE sich das mobile Gerät in den Werkszustand zurücksetzen. Es SOLLTEN dabei die Daten oder die Verschlüsselungsschlüssel sicher vernichtet werden. Es SOLLTE vermieden werden, dass die Benutzenden bei einem Passwortwechsel Kennworte nutzen, die erst vor Kurzem verwendet wurden.

SYS.3.2.1.A5 Updates von Betriebssystem und Apps (B)

Bereits bei der Auswahl von zu beschaffenden mobilen Geräten MUSS die Institution darauf achten, dass die herstellende Institution angibt, über welchen geplanten Nutzungszeitraum Sicherheitsaktualisierungen für die Geräte bereitgestellt werden. Ältere Geräte, für die keine Aktualisierungen mehr bereitgestellt werden, MÜSSEN ausgesondert und durch von der herstellenden Institution unterstützte Geräte ersetzt werden. Apps SOLLTEN ebenfalls NICHT mehr eingesetzt werden, wenn sie nicht mehr durch die herstellende Institution unterstützt werden.

SYS.3.2.1.A6 Datenschutzeinstellungen und Berechtigungen (B)

Der Zugriff von Apps und Betriebssystem auf Daten und Schnittstellen MUSS angemessen eingeschränkt werden. Die Datenschutzeinstellungen MÜSSEN so restriktiv wie möglich konfiguriert werden. Insbesondere der Zugriff auf Kamera, Mikrofon sowie Ortungs- und Gesundheits- bzw. Fitnessdaten MUSS auf Konformität mit den organisationsinternen Datenschutz- und Sicherheitsvorgaben überprüft werden. Der Zugriff MUSS restriktiv konfiguriert bzw. deaktiviert werden.

Sicherheitsrelevante Berechtigungseinstellungen MÜSSEN so festgelegt werden, dass sie nicht durch Benutzende oder Apps geändert werden können. Wo dies technisch nicht möglich ist, MÜSSEN die Berechtigungseinstellungen regelmäßig geprüft und erneut gesetzt werden. Dies gilt insbesondere auch nach der Installation von Updates.

SYS.3.2.1.A7 Verhaltensregeln bei Sicherheitsvorfällen (B) [Benutzende]

Gehen Geräte verloren oder werden unberechtigte Änderungen an Gerät und Software festgestellt, MÜSSEN die Benutzenden sofort die Zuständigen informieren.

SYS.3.2.1.A8 Installation von Apps (B)

Die Institution MUSS regeln, ob, wie und welche Apps Benutzende selbst auf ihren Geräten installieren dürfen. Sie SOLLTEN nur freigegebene Apps installieren dürfen. Die Institution MUSS festlegen, aus welchen Quellen Apps installiert werden dürfen. Es MUSS unterbunden werden, dass sich Apps aus nicht zugelassenen Quellen installieren lassen.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.3.2.1.A9 Restriktive Nutzung von funktionalen Erweiterungen (S)

Funktionale Erweiterungen SOLLTEN nur restriktiv genutzt werden. Wenn möglich, SOLLTE auf funktionale Erweiterungen verzichtet werden. Die funktionalen Erweiterungen SOLLTEN keinen automatischen Zugriff auf schützenswerte Informationen haben. Sie SOLLTEN die festgelegte Grundkonfiguration nicht umgehen oder ändern können.

SYS.3.2.1.A10 Richtlinie für Mitarbeitende zur Benutzung von mobilen Geräten (S) [Benutzende]

Eine verbindliche Richtlinie für Mitarbeitende zur Benutzung von mobilen Geräten SOLLTE erstellt werden. Diese SOLLTE festlegen, wie mobile Geräte genutzt und gepflegt werden sollen. Die Themen Aufbewahrung und Verlustmeldung SOLLTEN darin behandelt werden. Außerdem SOLLTE verboten werden, Verwaltungssoftware zu deinstallieren, das Gerät zu rooten oder sicherheitsrelevante Konfigurationen zu ändern.

SYS.3.2.1.A11 Verschlüsselung des Speichers (S)

Der nichtflüchtige Speicher des mobilen Geräts SOLLTE verschlüsselt werden. Schützenswerte Daten auf zusätzlich verwendeten Speichermedien, wie SD-Karten, SOLLTEN verschlüsselt werden.

SYS.3.2.1.A12 Verwendung nicht personalisierter Gerätenamen (S)

Der Gerätename SOLLTE keine Hinweise auf die Institution oder die Benutzenden enthalten.

SYS.3.2.1.A13 Regelungen zum Screensharing und Casting (S)

Es SOLLTE entschieden werden, ob und wie Funktionen zur Übertragung von Bildschirminhalten, Audio oder Video (Screensharing oder Casting) eingesetzt werden sollen. Die Funktionen SOLLTEN organisatorisch oder technisch geregelt werden. Hierzu SOLLTE eine entsprechende Vereinbarung mit den Benutzenden getroffen werden.

SYS.3.2.1.A14 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.1.A15 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.1.A16 Deaktivierung nicht benutzter Kommunikationsschnittstellen (S) [Benutzende]

Kommunikationsschnittstellen SOLLTEN nur bei Bedarf und nur in geeigneten Umgebungen aktiviert werden. Wird ein MDM verwendet, SOLLTEN die Schnittstellen zentral über das MDM verwaltet werden.

SYS.3.2.1.A17 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.1.A18 Verwendung biometrischer Authentisierung (S)

Wenn biometrische Verfahren zur Authentisierung (z. B. ein Fingerabdrucksensor) genutzt werden sollen, SOLLTE geprüft werden, ob dadurch ein ähnlich hoher oder höherer Schutz im Vergleich zu einem Gerätepasswort erzielt werden kann. Im Zweifelsfall oder bei einem schlechteren Schutz SOLLTEN biometrische Verfahren NICHT genutzt werden. Die Benutzenden SOLLTEN für die Fälschbarkeit von biometrischen Merkmalen sensibilisiert werden.

SYS.3.2.1.A19 Verwendung von Sprachassistenten (S)

Sprachassistenten SOLLTEN nur eingesetzt werden, wenn sie zwingend notwendig sind. Andernfalls SOLLTEN sie deaktiviert werden. Generell SOLLTE ein Sprachassistent nicht genutzt werden können, wenn das Gerät gesperrt ist.

SYS.3.2.1.A20 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.1.A21 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.1.A22 Einbindung mobiler Geräte in die interne Infrastruktur via VPN (S)

Mobile Endgeräte SOLLTEN nur mittels eines VPN in die Infrastruktur der Institution integriert werden. Hierzu SOLLTE ein geeignetes Verfahren ausgewählt und eingesetzt werden. Statt durch Passwörter SOLLTEN sich die Geräte über Zertifikate gegenüber der internen Infrastruktur authentisieren.

SYS.3.2.1.A28 Verwendung der Filteroption für Webseiten (S)

Wird in der Institution bereits ein Reputationsdienst oder ein entsprechender Proxy-Server verwendet, SOLLTE dieser als globaler HTTP-Proxy für alle installierten Browser hinterlegt werden. Ist der Proxy nur im internen Netz erreichbar, SOLLTEN die Endgeräte über eine VPN-Verbindung wahlweise permanent oder basierend auf den verwendeten Apps geeignet eingebunden werden.

Sind die mobilen Endgeräte nicht in eine vorhandene Proxy- oder Reputations-Infrastruktur der Institution eingebunden, SOLLTEN für Webbrowser Filteroptionen auf Basis von Allowlists oder Blocklists oder Inhaltsfilter Dritter verwendet werden.

SYS.3.2.1.A31 Regelung zu Mobile Payment (S)

Es SOLLTE geregelt werden, ob Mobile Payment mit dienstlichen Smartphones und Tablets erlaubt wird.

SYS.3.2.1.A32 MDM Nutzung (S)

Smartphones und Tablets SOLLTEN durch ein MDM-System verwaltet werden.

SYS.3.2.1.A33 Auswahl und Installation von Sicherheits-Apps (S)

Alle mobilen Endgeräte SOLLTEN vor Schadprogrammen geschützt werden. Falls möglich, SOLLTEN für das Endgerät geeignete Sicherheits-Apps ausgewählt werden. Die Sicherheits-Apps SOLLTEN automatisch, zum Beispiel durch ein MDM, installiert werden.

SYS.3.2.1.A34 Konfiguration des verwendeten DNS-Servers (S)

Standard-Gateway-Einträge, wie beispielsweise DNS-Server der herstellenden oder entwickelnden Institutionen, SOLLTEN durch die des Providers oder durch eigene ersetzt werden.

Sollte der Provider sogenanntes DNS-over-HTTPS (DoH) anbieten, SOLLTE dieses verwendet werden. Bietet er es noch nicht an, SOLLTE es deaktiviert werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.3.2.1.A23 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.3.2.1.A24 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.3.2.1.A25 Nutzung von getrennten Arbeitsumgebungen (H)

Ist es den Mitarbeitenden erlaubt, dienstliche Geräte auch privat zu nutzen, SOLLTEN Lösungen für getrennte Arbeitsumgebungen auf dem Endgerät eingesetzt werden. Wenn möglich, SOLLTEN dafür nur zertifizierte Produkte (z. B. nach Common Criteria) beschafft werden. Dienstliche Daten SOLLTEN ausschließlich in der dienstlichen Umgebung verbleiben.

SYS.3.2.1.A26 Nutzung von PIM-Containern (H)

Informationen auf den mobilen Endgeräten SOLLTEN gekapselt werden, zum Beispiel in einem PIM-Container. Zusätzlich SOLLTEN die Daten durch eine separate Authentisierung und eine vom Betriebssystem unabhängige Daten- und Transportverschlüsselung abgesichert werden.

SYS.3.2.1.A27 Einsatz besonders abgesicherter Endgeräte (H)

Institutionen SOLLTEN abhängig vom Schutzbedarf besonders abgesicherte mobile Endgeräte einsetzen, die für die Verarbeitung von Informationen nach gesetzlichen Informationsschutz-Klassifizierungen zertifiziert sind.

SYS.3.2.1.A29 Verwendung eines institutionsbezogenen APN (H)

Es SOLLTE geprüft werden, ob ein institutionsbezogener Zugangspunkt zum Mobilfunknetz (APN, Access Point Name) zur Eingrenzung des erlaubten Geräte-Pools verwendet werden kann. Alle Geräte, die diesen APN verwenden, SOLLTEN vom Mobilfunk-Provider einen mit der Institution abgestimmten IP-Adressbereich erhalten. Für die Authentisierung SOLLTE ein komplexes Passwort mit maximal 64 Stellen mit dem Mobilfunk-Provider vereinbart werden. Beim Einsatz eines institutionsbezogenen APN SOLLTE die Authentisierung auf Basis des Protokolls CHAP realisiert werden.

SYS.3.2.1.A30 Einschränkung der App-Installation mittels Allowlist (H)

Bei erhöhtem Schutzbedarf SOLLTEN auf den mobilen Endgeräten nur freigegebene und geprüfte Apps installiert werden dürfen. Wird ein MDM eingesetzt, SOLLTE es verhindern, dass andere Apps installiert werden oder alternativ unbefugt installierte Apps sofort wieder entfernen.

SYS.3.2.1.A35 Verwendung einer Firewall (H)

Auf Smartphones und Tablets SOLLTE eine Firewall installiert und aktiviert sein.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013, insbesondere in Annex A, A.6.2 „Mobile devices and teleworking", Vorgaben für den Einsatz von mobilen Endgeräten.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security", insbesondere in Area PA2 Mobile Computing, Vorgaben für den Einsatz von mobilen Endgeräten.

Das National Institute of Standards and Technology (NIST) stellt folgende Dokumente im Bereich mobile Endgeräte bereit:

- „Guidelines for Managing the Security of Mobile Devices in the Enterprise: NIST Special Publication 800-124", Revision 1, Juni 2013
- „Security and Privacy Controls for Federal Information Systems and Organizations: NIST Special Publication 800-53", Revision 4, April 2013
- „Securing Electronic Health Record on Mobile Devices: NIST Special Publication 1800-1d", Draft, Juli 2015

Bundesamt
für Sicherheit in der
Informationstechnik

SYS.3.2.2 Mobile Device Management (MDM)

1. Beschreibung

1.1. Einleitung

Smartphones, Tablets und Phablets sind für viele Mitarbeitende ein nicht mehr wegzudenkender Teil ihrer Arbeit. Der IT-Betrieb muss jedoch immer mehr solcher Geräte in vielen unterschiedlichen Ausführungen bereitstellen und dabei gleichzeitig für eine angemessene Sicherheit sorgen. Hinzu kommt, dass mobile Endgeräte (Mobile Devices) besonderen Gefahren ausgesetzt sind und die Administration sich in grundlegenden Punkten von anderen IT-Systemen unterscheidet.

Deswegen ist ein Mobile Device Management (MDM) besonders in Institutionen mit einer größeren Anzahl von Smartphones, Tablets und Phablets unabdingbar für einen geregelten und sicheren Betrieb dieser Geräte. Mit einer entsprechenden Software für das MDM können die Endgeräte zentral verwaltet werden, es lassen sich Sicherheitsregeln durchsetzen und es können Notfallaktionen ausgelöst werden. Ein MDM gewährleistet somit auf allen Geräten einen gleichen oder zumindest vergleichbaren Sicherheitsstandard.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, aufzuzeigen, wie mit einem MDM mobile Endgeräte sicher von Institutionen genutzt werden können. Er gibt zudem Hinweise zum Betrieb eines MDM.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.3.2.2 *Mobile Device Management (MDM)* ist für den Informationsverbund einzusetzen, wenn mobile Endgeräte mit einem Mobile Device Management (MDM) verwaltet werden.

Mobile Endgeräte (Mobile Devices) im Sinne dieses Bausteins sind Smartphones, Tablets und Phablets, auf denen mobile Betriebssysteme wie Android oder iOS installiert sind. Die Sicherheitsanforderungen von Smartphones, Tablets, Notebooks und Tablets mit Desktop-Betriebssystemen werden in anderen Bausteinen der Schicht SYS *IT-Systeme* beschrieben. Die Anforderungen aus SYS.3.2.1 *Allgemeine Smartphones und Tablets* müssen ebenfalls berücksichtigt werden, wenn ein MDM verwendet wird. Wie die Smartphones, Tablets und Phablets spezifisch abgesichert werden, wird zusätzlich detailliert in den Bausteinen für die jeweiligen Betriebssysteme beschrieben, z. B. in SYS.3.2.3 *iOS (for Enterprise)* oder SYS.3.2.4 *Android*.

Für das MDM muss ein Berechtigungskonzept erstellt werden. Anforderungen dazu stellt der Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* auf. Eine der ureigensten Aufgaben eines MDM ist die Administration von mobilen Endgeräten. Sicherheitsanforderungen für Administrationen enthält der Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration*.

Nicht behandelt werden in diesem Baustein Aspekte von „Bring your own device“ (BYOD).

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.3.2.2 *Mobile Device Management (MDM)* von besonderer Bedeutung:

2.1. Keine ausreichende Synchronisation mit dem MDM

Damit das MDM die von den Zuständigen definierten Regelungen auf den mobilen Endgeräten durchsetzen kann, müssen die Geräte regelmäßig mit dem MDM synchronisiert werden. Wenn ein Gerät über einen längeren Zeitraum nicht mit dem MDM verbunden ist, können beispielsweise neue oder aktualisierte Regelungen nicht aufgespielt werden. Auch können, wenn zu einem verlorenen Gerät keine Verbindung besteht, die Daten nicht mehr aus der Ferne gelöscht werden.

2.2. Fehlerhafte Administration des MDM

MDM-Lösungen sind komplexe Anwendungen mit typischerweise mehreren Hundert unterschiedlichen Regeln. Nicht alle Regeln sind dabei miteinander kombinierbar und umgekehrt hängen viele Regeln voneinander ab. Durch Fehler bei der Administration können sowohl das MDM als auch die Endgeräte diversen Gefahren ausgesetzt sein, die sich direkt oder indirekt auf die Vertraulichkeit, Verfügbarkeit oder Integrität der Daten und Anwendungen auswirken.

2.3. Ungeeignetes Rechtemanagement im MDM

Das Rechtemanagement des MDM entscheidet, welche Benutzenden welche Einstellungen auf den mobilen Geräten vornehmen dürfen und wer auf welche Daten zugreifen darf. Wenn Benutzenden eine falsche Rolle zugeordnet wird, besteht die Gefahr, dass ihnen zu hohe Rechte eingeräumt werden. So könnten sie beispielsweise Daten unbefugt einsehen oder Einstellungen am Gerät verändern. Auch wäre es möglich, dass sie Apps installieren und benutzen, die in der Institution nicht zugelassen sind, beispielsweise zur Nutzung von Cloud-Speicherdiensten. Dadurch können schützenswerte Daten aus der Institution abfließen oder es wird gegen die gesetzlichen Datenschutzbestimmungen verstoßen.

2.4. Unberechtigte Erstellung von Bewegungsprofilen durch das MDM

Mit den meisten MDM-Produkten lässt sich ermitteln, wo sich ein Gerät gerade befindet, und es können standortabhängig Daten oder Apps freigegeben bzw. gesperrt werden (sogenanntes „Geofencing"). Dadurch entstehen detaillierte Bewegungsprofile der Geräte und somit auch der Benutzenden. Werden diese Daten erhoben, ohne die Benutzenden in geeigneter Weise darüber zu informieren, verstoßen die Verantwortlichen unter Umständen gegen datenschutzrechtliche Bestimmungen. Auch besteht die Gefahr, dass im Falle eines Angriffs diese Daten an Unbefugte gelangen. Ebenso kann Geofencing dazu missbraucht werden, um Mitarbeitende unzulässig zu kontrollieren.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.3.2.2 *Mobile Device Management (MDM)* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.3.2.2.A1 Festlegung einer Strategie für das Mobile Device Management (B)

Es MUSS eine Strategie erarbeitet werden, die festlegt, wie Mitarbeitende mobile Endgeräte benutzen dürfen und wie die Geräte in die IT-Strukturen der Institution integriert sind. Grundlage MUSS dabei der Schutzbedarf der zu verarbeitenden Informationen sein. Die Strategie MUSS mindestens folgende Aspekte abdecken:

- Darf das MDM als Cloud-Dienst betrieben werden?
- Soll das MDM durch die Institution selbst betrieben werden?
- Soll das MDM alle Apps bereitstellen oder dürfen die Benutzenden selber Apps installieren? Welche Restriktionen gibt die Institution bei bereitgestellten oder selbst installierten Apps vor?
- Soll das MDM in eine weitere Infrastruktur eingebunden werden?
- Welche Anforderungen bezüglich Supportleistungen und Reaktionszeiten sind an die anbietende Institution des MDM zu stellen?
- Welche Compliance-Anforderungen müssen durchgesetzt werden?
- Welche mobilen Geräte und welche Betriebssysteme muss das MDM unterstützen?
- Muss die MDM-Lösung mandantenfähig sein? Gewährleistet sie die notwendige Mandantentrennung?
- Müssen Cloud-Dienste eingebunden werden?
- Müssen Dokumentenmanagementsysteme eingebunden werden?
- Muss das MDM auch Peripheriegeräte einbinden und verwalten?
- Welches Betriebsmodell soll eingesetzt werden: private Endgeräte (Bring Your Own Device, BYOD), personalisierte Endgeräte (Eigentum der Institution) oder nicht personalisierte Endgeräte (Eigentum der Institution, gemeinsam genutzt)?

Die Strategie MUSS schriftlich fixiert und von dem oder der ISB freigegeben werden.

SYS.3.2.2.A2 Festlegung erlaubter mobiler Endgeräte (B)

Es MUSS festgelegt werden, welche mobilen Endgeräte und Betriebssysteme in der Institution zugelassen sind. Alle erlaubten Geräte und Betriebssysteme MÜSSEN den Anforderungen der MDM-Strategie genügen und die technischen Sicherheitsanforderungen der Institution vollständig erfüllen. Das MDM MUSS so konfiguriert werden, dass nur mit freigegebenen Geräten auf Informationen der Institution zugegriffen werden kann. Es DÜRFEN nur von der Institution zugelassene mobile Endgeräte beschafft werden.

SYS.3.2.2.A3 Auswahl eines MDM-Produkts (B)

Wenn eine geeignete MDM-Software beschafft werden soll, MUSS sichergestellt sein, dass sich mit ihr alle in der MDM-Strategie festgelegten Anforderungen erfüllen lassen. Auch MUSS sie sämtliche technischen und organisatorischen Sicherheitsmaßnahmen umsetzen können und alle zugelassenen mobilen Endgeräte unterstützen.

SYS.3.2.2.A4 Verteilung der Grundkonfiguration auf mobile Endgeräte (B)

Alle mobilen Endgeräte MÜSSEN, bevor sie eingesetzt werden, in das MDM integriert werden. Wenn die Geräte die Grundkonfiguration erhalten, MÜSSEN sie sich im Werkszustand befinden. Die Verbindung der mobilen Endgeräte zum MDM MUSS angemessen abgesichert werden. Bei bereits benutzten Geräten MÜSSEN vorher alle institutionsbezogenen Daten gelöscht werden. Ein nicht über MDM konfiguriertes Endgerät DARF NICHT auf Informationen der Institution zugreifen können.

SYS.3.2.2.A5 Installation des MDM-Clients (B)

Wenn mobile Endgeräte an Mitarbeitende übergeben werden, MUSS, wenn vom Betriebssystem nicht bereits bereitgestellt, darauf der MDM-Client installiert und konfiguriert sein.

SYS.3.2.2.A20 Regelmäßige Überprüfung des MDM (B)

Sicherheitseinstellungen MÜSSEN regelmäßig überprüft werden. Bei neuen Betriebssystemversionen der mobilen Endgeräte MUSS vorab geprüft werden, ob das MDM diese vollständig unterstützt und die Konfigurationsprofile und Sicherheitseinstellungen weiterhin wirksam und ausreichend sind. Abweichungen MÜSSEN korrigiert werden. Die zugeteilten Berechtigungen für Benutzende und Administrierende MÜSSEN regelmäßig daraufhin überprüft werden, ob sie weiterhin angemessen sind (Minimalprinzip).

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.3.2.2.A6 Protokollierung des Gerätestatus (S)

Der Lebenszyklus einschließlich der Konfigurationshistorie eines mobilen Endgerätes SOLLTE ausreichend protokolliert und zentral abrufbar sein. Bei Bedarf SOLLTE der aktuelle Status der verwalteten Endgeräte durch den IT-Betrieb ermittelt werden können (Device Audit).

SYS.3.2.2.A7 Installation von Apps (S)

Apps SOLLTEN gemäß den Anforderungen des geplanten Einsatzszenarios über das MDM installiert, deinstalliert und aktualisiert werden. Das MDM SOLLTE die Installation, Deinstallation und Aktualisierung erzwingen, sobald eine Verbindung zum mobilen Endgerät besteht. Über das MDM installierte Apps SOLLTEN NICHT durch Benutzende deinstalliert werden können. Das MDM SOLLTE eine Block- oder Allow-List für die Installation von Apps ermöglichen.

SYS.3.2.2.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.2.A9 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.2.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.2.A11 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.2.A12 Absicherung der MDM-Betriebsumgebung (S)

Das MDM selbst SOLLTE durch technische Maßnahmen abgesichert werden, um dem Schutzbedarf der hinterlegten oder verarbeiteten Informationen zu genügen. Das zugrundeliegende Betriebssystem SOLLTE gehärtet werden.

SYS.3.2.2.A21 Verwaltung von Zertifikaten (S)

Zertifikate zur Nutzung von Diensten auf dem mobilen Endgerät SOLLTEN zentral über das MDM installiert, deinstalliert und aktualisiert werden. Die Installation von nicht vertrauenswürdigen und nicht verifizierbaren (Root-) Zertifikaten durch Benutzende SOLLTE durch das MDM verhindert werden. Das MDM SOLLTE Mechanismen unterstützen, um die Gültigkeit von Zertifikaten zu überprüfen.

SYS.3.2.2.A22 Fernlöschung und Außerbetriebnahme von Endgeräten (S)

Das MDM SOLLTE sicherstellen, dass sämtliche dienstliche Daten auf dem mobilen Endgerät aus der Ferne gelöscht werden können (Remote Wipe bei bestehender Datenverbindung). Werden in dem mobilen Endgerät externe Speicher genutzt, SOLLTE geprüft werden, ob diese bei einem Remote Wipe ebenfalls gelöscht werden sollen. Diese Funktion SOLLTE vom MDM unterstützt werden.

Der Prozess zur Außerbetriebnahme des mobilen Endgerätes (Unenrollment) SOLLTE sicherstellen, dass keine schutzbedürftigen Daten auf dem mobilen Endgerät oder eingebundenen Speichermedien verbleiben. Dies SOLLTE insbesondere dann gelten, wenn das Unenrollment aus der Ferne ausgeführt wird.